

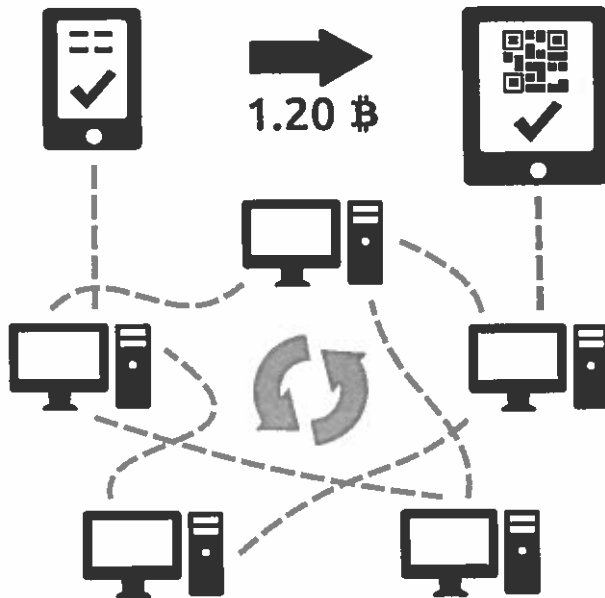
Exhibit B

How does Bitcoin work?

This is a question that often causes confusion. Here's a quick explanation!

The basics for a new user

As a new user, you can get started with Bitcoin without understanding the technical details. Once you have installed a Bitcoin wallet on your computer or mobile phone, it will generate your first Bitcoin address and you can create more whenever you need one. You can disclose your addresses to your friends so that they can pay you or vice versa. In fact, this is pretty similar to how email works, except that Bitcoin addresses should only be used once.



Balances - block chain

The block chain is a **shared public ledger** on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

Transactions - private keys

A transaction is a **transfer of value between Bitcoin wallets** that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a *private key* or *seed*, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The *signature* also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called *mining*.

Processing - mining

Mining is a **distributed consensus system** that is used to *confirm* waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a *block* that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

Going down the rabbit hole

This is only a very short and concise summary of the system. If you want to get into the details, you can read the original paper that describes the system's design, read the developer documentation, and explore the Bitcoin wiki.